

FIG.1

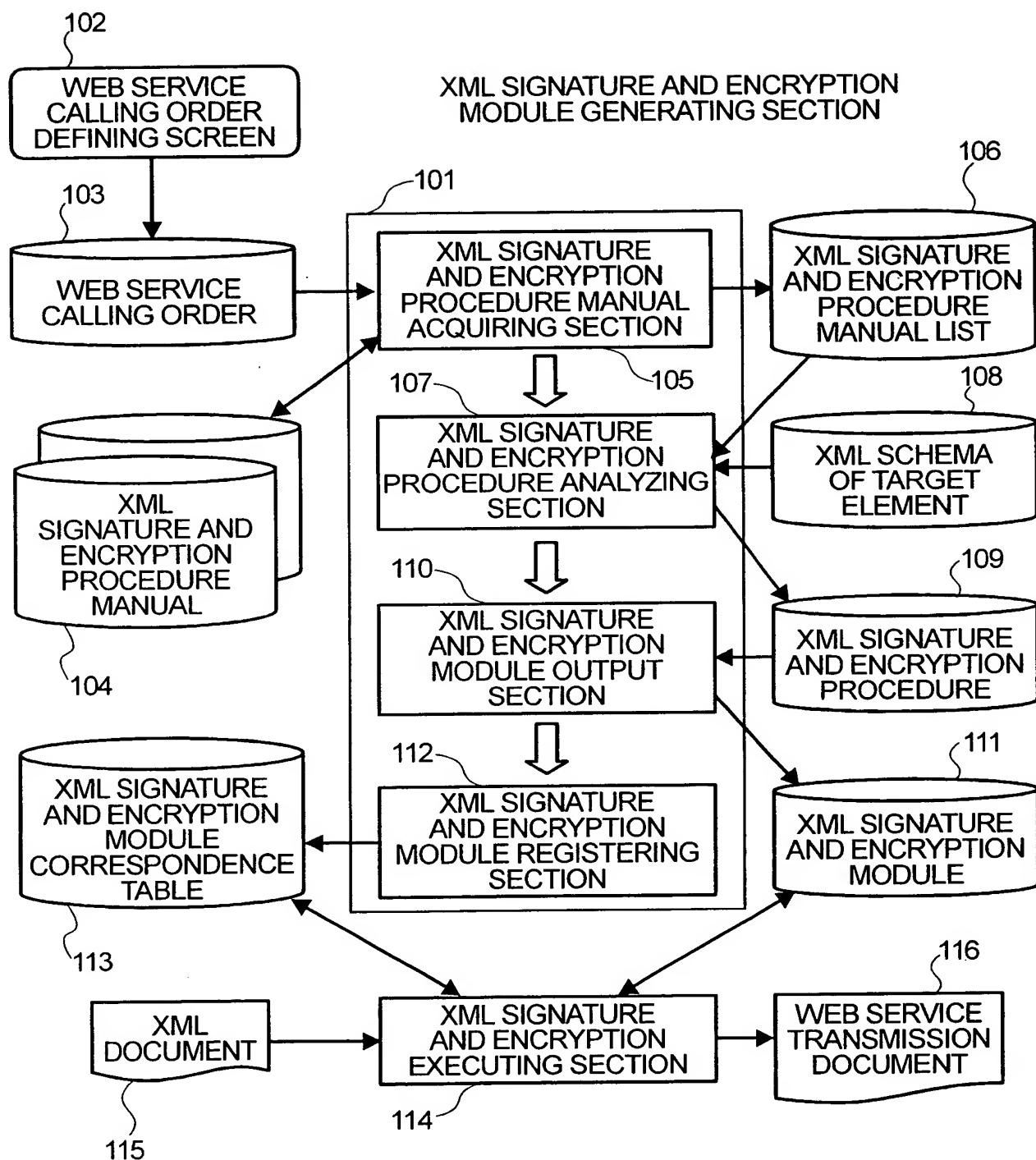


FIG.2

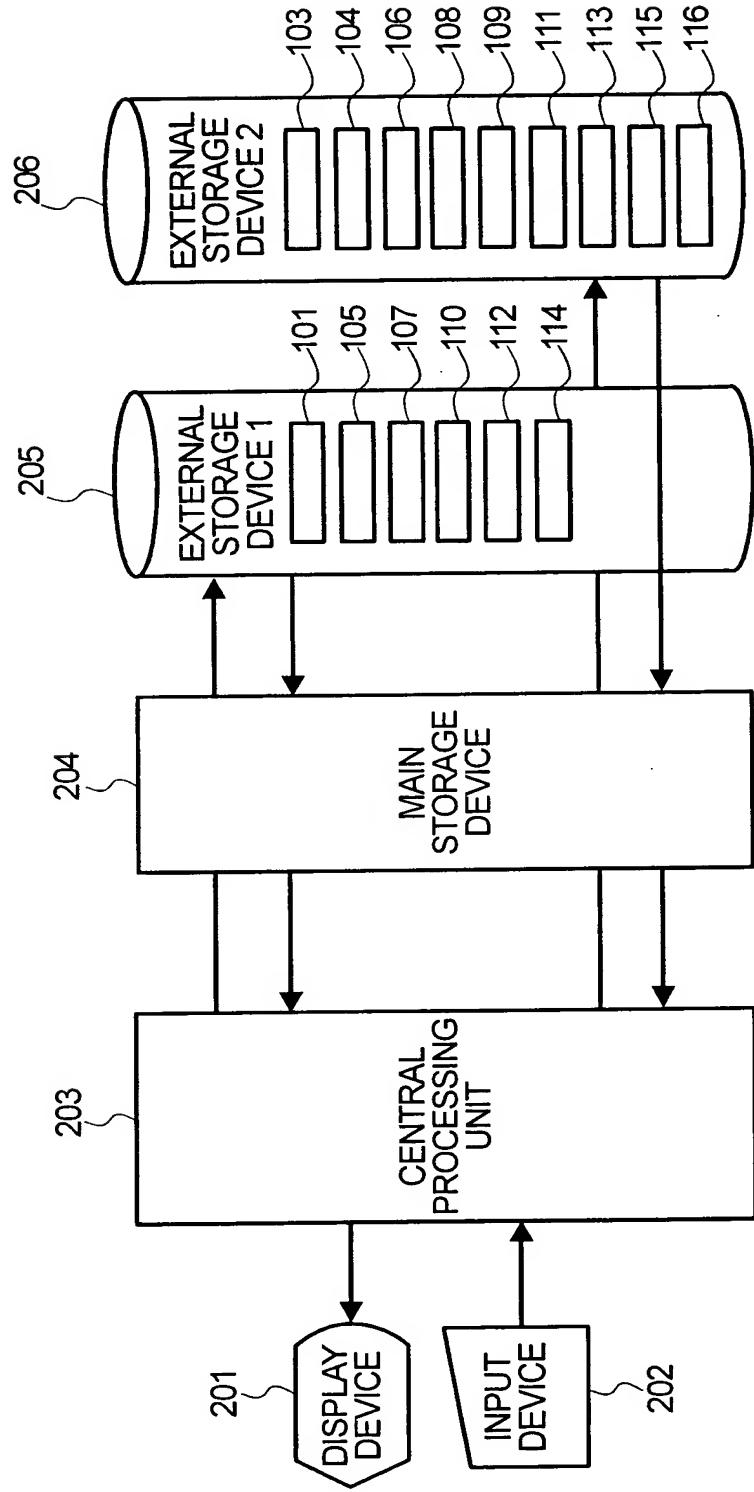


FIG.3

WEB SERVICE CALLING ORDER DEFINING SCREEN 102

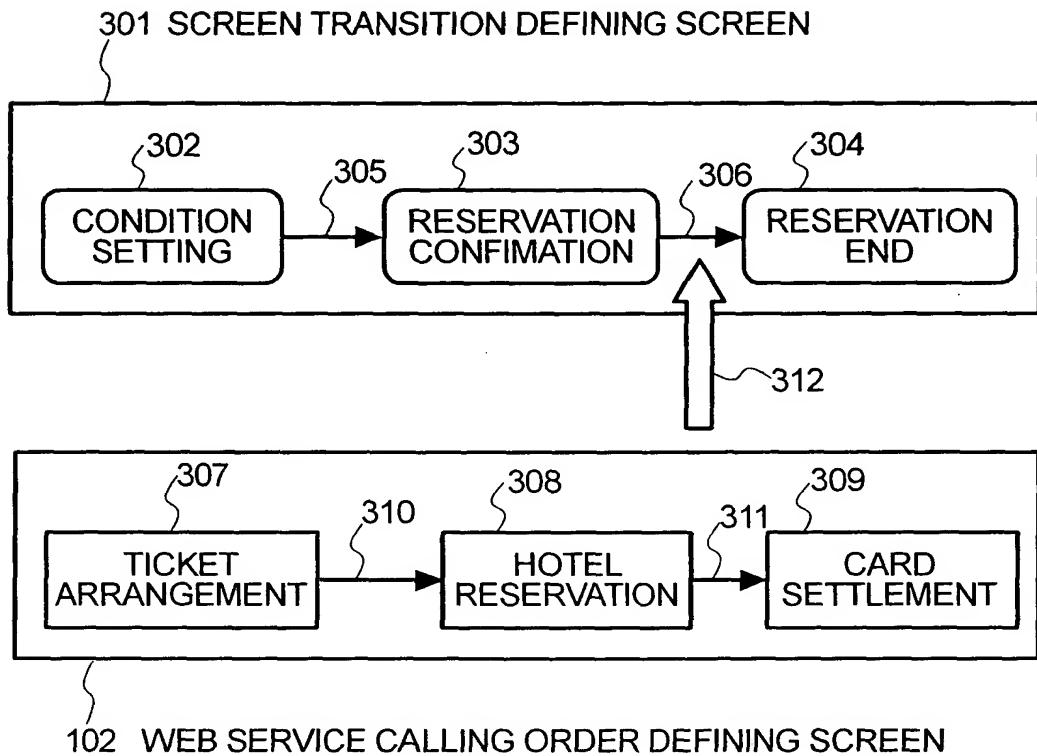


FIG.4

WEB SERVICE CALLING ORDER 103

401	402	403	404	405
ID	NEXT ID	NAME	WEB SERVICE URI	XML SIGNATURE AND ENCRYPTION PROCEDURE MANUAL URI
A	B	TICKET ARRANGEMENT	http://www.tickets.com/	http://www.tickets.com/sec
B	C	HOTEL RESERVATION	http://www.hotels.com/	http://www.hotels.com/sec
C	NONE	CARD SETTLEMENT	http://www.cards.com/	http://www.cards.com/sec

FIG.5

XML SIGNATURE AND ENCRYPTION PROCEDURE MANUAL 104

XML SIGNATURE AND ENCRYPTION PROCEDURE MANUAL 501 CORRESPONDING TO 406

	ORDER	TARGET ELEMENT	OPERATION	ALGORITHM
508	1	tickets	ENCRYPTION	AES
509	2	userinfo	ENCRYPTION	DESede
510	3	root	SIGNATURE	DSS

XML SIGNATURE AND ENCRYPTION PROCEDURE MANUAL 502 CORRESPONDING TO 407

	ORDER	TARGET ELEMENT	OPERATION	ALGORITHM
511	1	hotels	ENCRYPTION	DESede
512	2	userinfo	ENCRYPTION	AES
513	3	root	SIGNATURE	RSA

XML SIGNATURE AND ENCRYPTION PROCEDURE MANUAL 503 CORRESPONDING TO 408

	ORDER	TARGET ELEMENT	OPERATION	ALGORITHM
514	1	cardinfo	ENCRYPTION	RSA
515	2	userinfo	SIGNATURE	DSS

FIG.6

XML SIGNATURE AND ENCRYPTION PROCEDURE MANUAL ACQUIRING SECTION 105

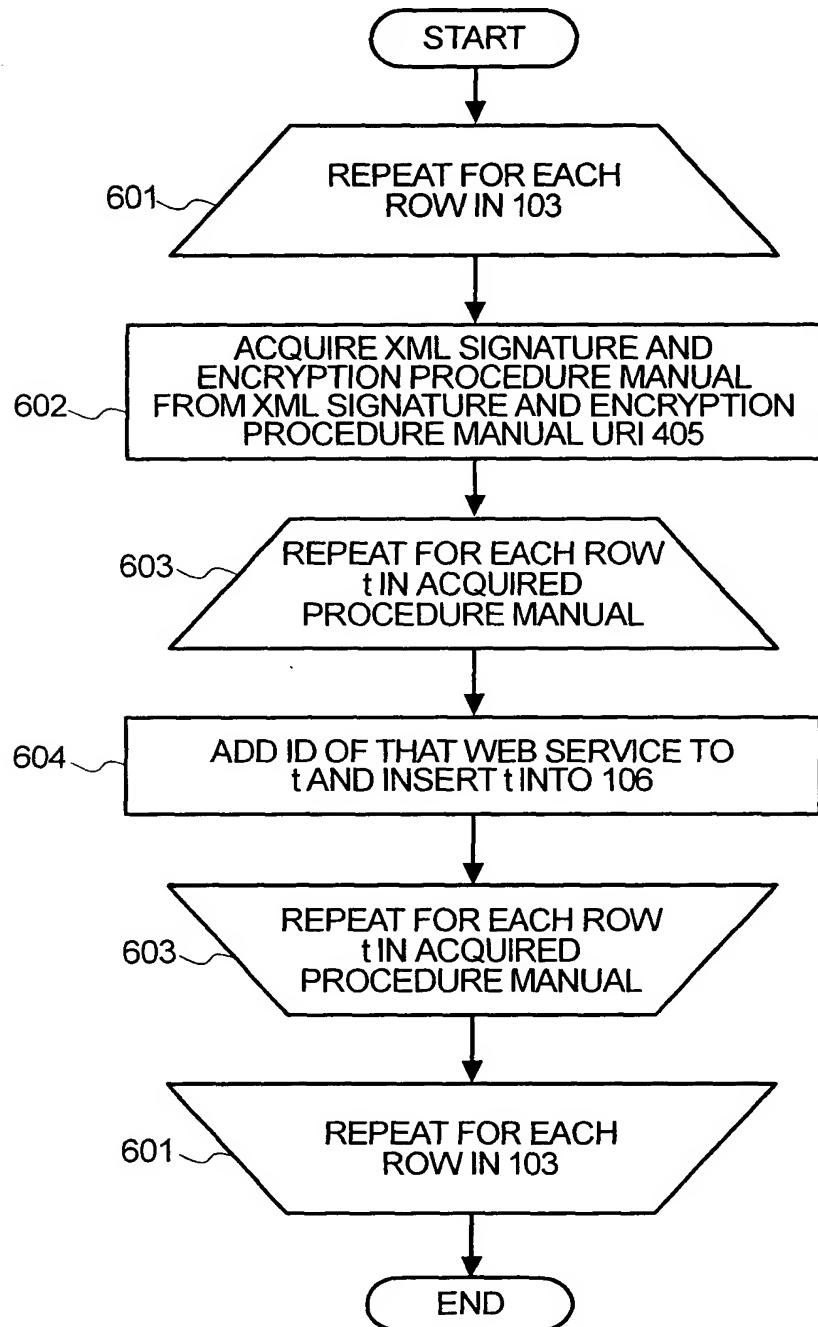


FIG.7

XML SIGNATURE AND ENCRYPTION PROCEDURE MANUAL LIST 106

	ID	ORDER	TARGET ELEMENT	OPERATION	ALGORITHM
706	A	1	tickets	ENCRYPTION	AES
707	A	2	userinfo	ENCRYPTION	DESede
708	A	3	root	SIGNATURE	DSS
709	B	1	hotels	ENCRYPTION	DESede
710	B	2	userinfo	ENCRYPTION	AES
711	B	3	root	SIGNATURE	RSA
712	C	1	cardinfo	ENCRYPTION	RSA
713	C	2	userinfo	SIGNATURE	DSS

FIG.8

XML SCHEMA 108 OF TARGET ELEMENT

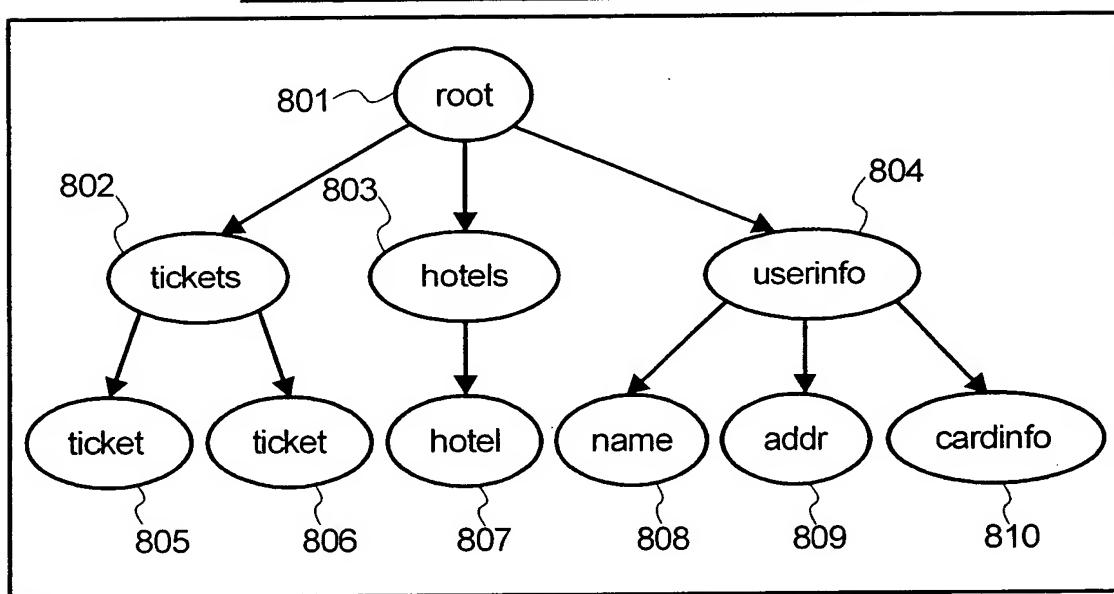


FIG.9

XML SIGNATURE AND ENCRYPTION
PROCEDURE ANALYZING SECTION 107

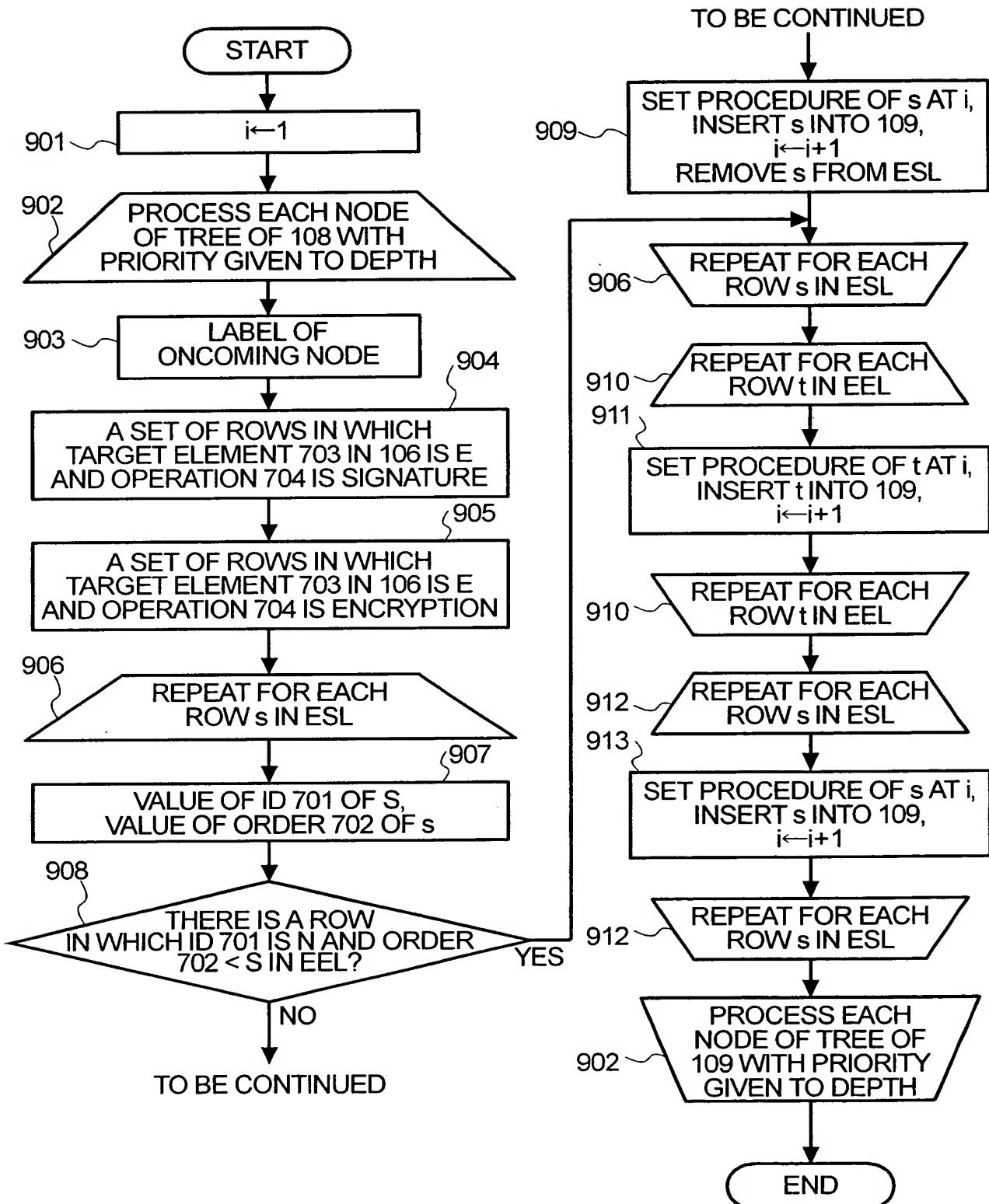


FIG.10

XML SIGNATURE AND ENCRYPTION PROCEDURE 109

	1001	1002	1003	1004	1005	1006
	PROCEDURE	ID	ORDER	TARGET ELEMENT	OPERATION	ALGORITHM
1007	1	A	1	tickets	ENCRYPTION	AES
1008	2	B	1	hotels	ENCRYPTION	DESede
1009	3	C	1	cardinfo	ENCRYPTION	RSA
1010	4	C	2	userinfo	SIGNATURE	DSS
1011	5	A	2	userinfo	ENCRYPTION	DESede
1012	6	B	2	userinfo	ENCRYPTION	AES
1013	7	A	3	root	SIGNATURE	DSS
1014	8	B	3	root	SIGNATURE	RSA

FIG.11

XML SIGNATURE AND ENCRYPTION MODULE OUTPUT SECTION 110

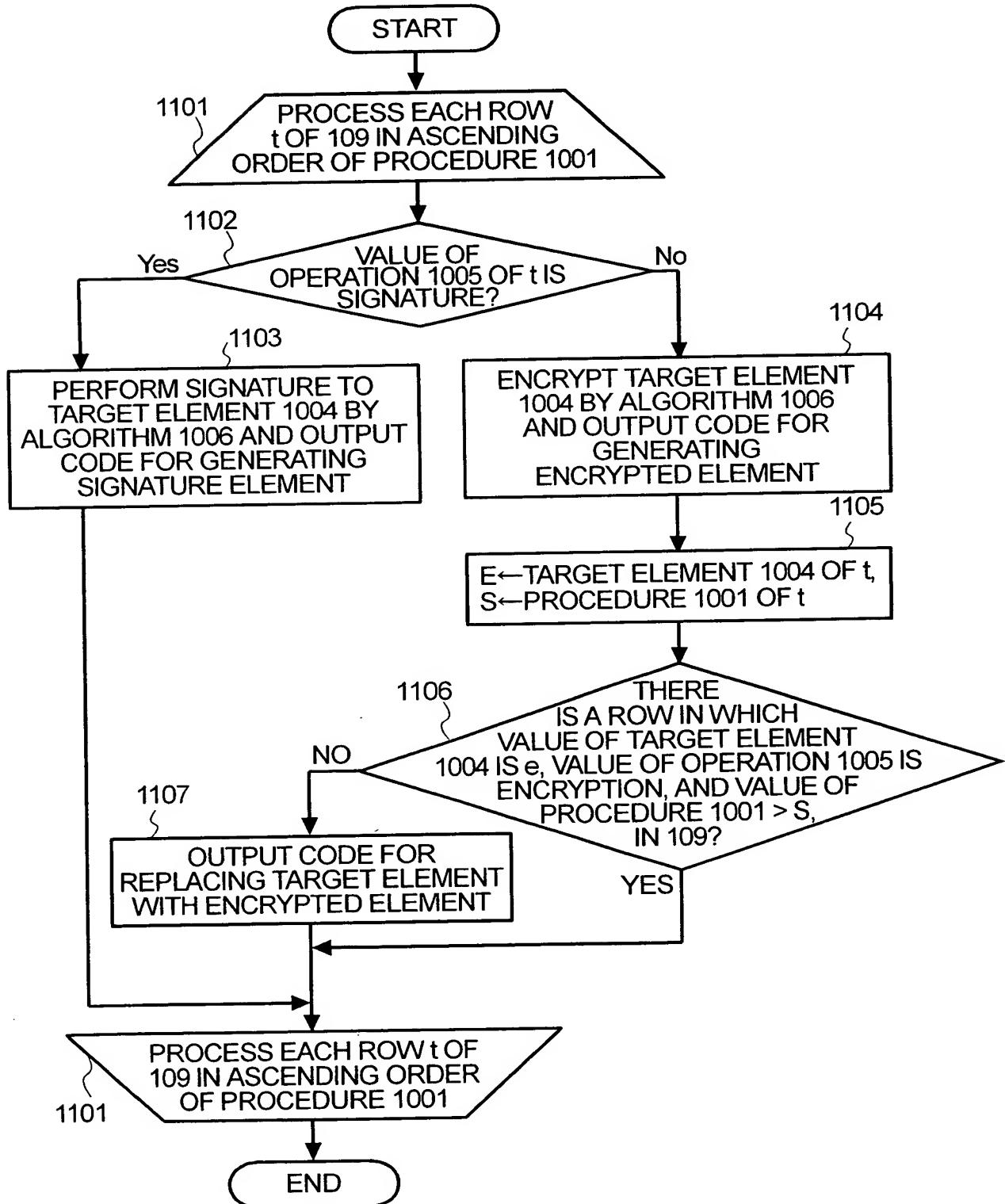


FIG.12

XML SIGNATURE AND ENCRYPTION MODULE111

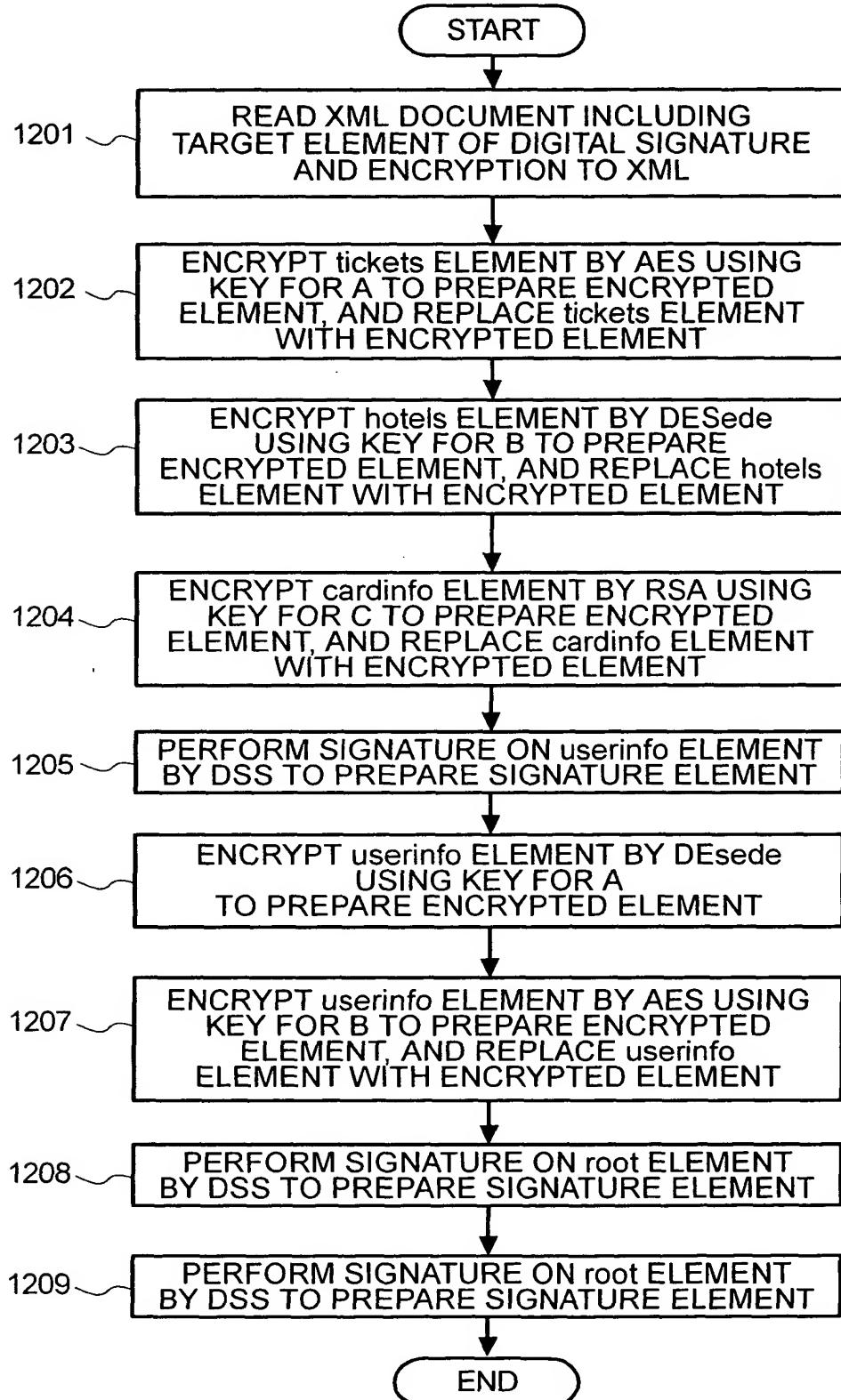


FIG.13

XML SIGNATURE AND ENCRYPTION MODULE
REGISTERING SECTION 112

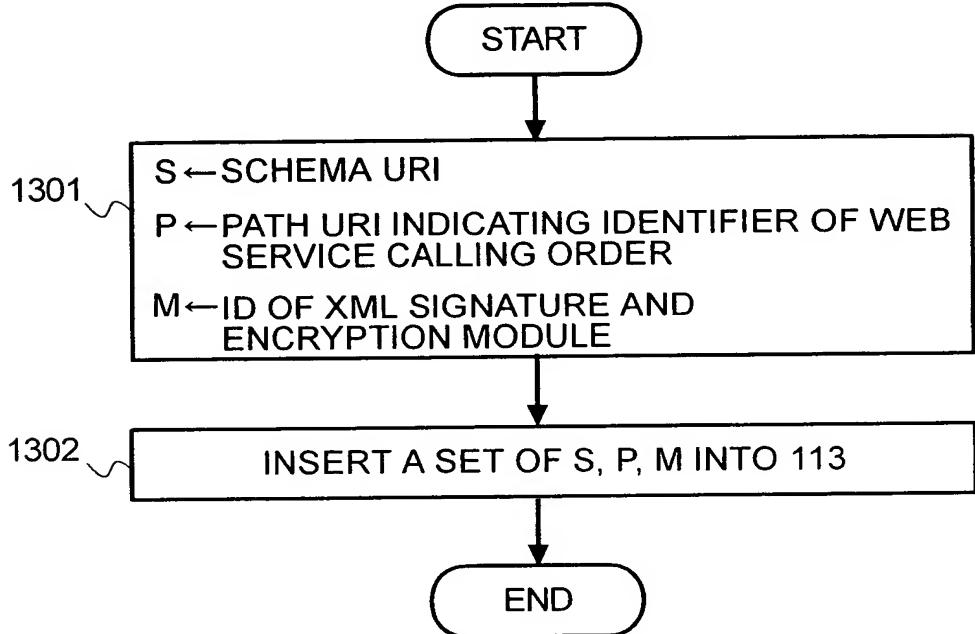


FIG.14

XML SIGNATURE AND ENCRYPTION
MODULE CORRESPONDENCETABLE 113

	SCHEMA URI	PATH URI	MODULE ID
1404	http://www.hitachi.co.jp/travel	http://www.hitachi.co.jp/tp1	XMLSEC01
1405	http://www.hitachi.co.jp/travel	http://www.hitachi.co.jp/tp2	XMLSEC02
1406	http://www.hitachi.co.jp/travel	http://www.hitachi.co.jp/bp	XMLSEC03
1407	http://www.hitachi.co.jp/travel	http://www.hitachi.co.jp/pp	XMLSEC04

FIG.15

XML SIGNATURE AND ENCRYPTION EXECUTING SECTION 114

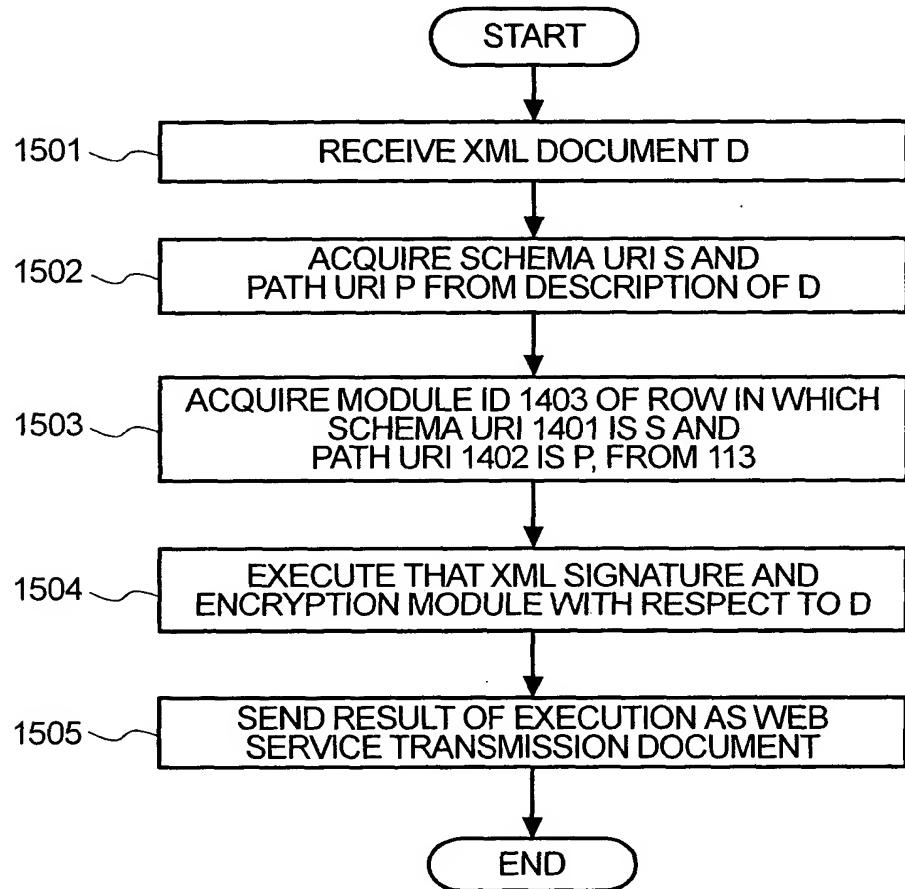


FIG.16

XML DOCUMENT 115

```
<?xml version="1.0" encoding="Shift_JIS"?>
<message>
  <path xmlns="http://www.hitachi.co.jp/tp" 1">
    <next URI="http://www.tickets.com/" />
    <next URI="http://www.hotels.com/" />
    <next URI="http://www.cards.com/" />
  </path>
  <root xmlns="http://www.hitachi.co.jp/travel">
    <tickets>
      <ticket from="TOKYO" to="OSAKA" date="02/04/01" time="09:00" />
      <ticket from="OSAKA" to="TOKYO" date="02/04/02" time="17:00" />
    </tickets>
    <hotels>
      <hotel name="HITACHI HOTEL" roomtype="S" date="02/04/01" />
    </hotels>
    <userinfo>
      <name>TARO HITACHI</name>
      <addr>CHIYODA-KU, TOKYO</addr>
      <cardinfo expiration="04/04" cardnumber="0123 4567 8901 2345" />
    </userinfo>
  </root>
</message>
```

FIG.17

WEB SERVICE TRANSMISSION DOCUMENT 116

```
<?xml version="1.0" encoding="Shift_JIS"?>
<message>
    <path xmlns="http://www.hitachi.co.jp/tp_1">
        <next URI="http://www.tickets.com/" />
        <next URI="http://www.hotels.com/" />
        <next URI="http://www.cards.com/" />
    </path>
    <root xmlns="http://www.hitachi.co.jp/travel">
        <EncryptedData xmlns="http://.../xmlenc#" Recipient="TICKET ARRANGEMENT">
            <CipherData><CipherValue>AB...CD</CipherValue></CipherData>
        <EncryptedData >
            <EncryptedData xmlns="http://.../xmlenc#" Recipient="HOTEL RESERVATION">
                <CipherData><CipherValue>EF...GH</CipherValue></CipherData>
            </EncryptedData >
            <EncryptedData xmlns="http://.../xmlenc#" Recipient="TICKET ARRANGEMENT">
                <CipherData><CipherValue>HI...JK</CipherValue><\CipherData>
            </EncryptedData >
            <EncryptedData xmlns="http://.../xmlenc#" Recipient="HOTEL RESERVATION">
                <CipherData><CipherValue>LM...NO</CipherValue></CipherData>
            </EncryptedData >
        </root >
        <Signature xmlns="http://.../xmldsig#" Id="TICKET ARRANGEMENT">
            <Signature Value>ABC...DEF</SignatureValue>
        </Signature>
        <Signature xmlns="http://.../xmldsig#" Id="HOTEL RESERVATION">
            <SignatureValue>BCD...EFG</SignatureValue>
        </Signature>
        <Signature xmlns="http://.../xmldsig#" ID="CARD SETTLEMENT">
            <SignatureValue>CDE...FGH</SignatureValue>
        </Signature>
    </message>
```

FIG.18

